HP OpenView Select Identity

Connector for
IBM Lotus Notes/Domino,
Versions 5.0.8, 5.0.10, 6.0.3, and 6.5.1

Installation Guide

Software Version: 3.0.1

October 2004

Legal Notices

Warranty

Hewlett-Packard makes no warranty of any kind with regard to this document, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. Hewlett-Packard shall not be held liable for errors contained herein or direct, indirect, special, incidental or consequential damages in connection with the furnishing, performance, or use of this material.

A copy of the specific warranty terms applicable to your Hewlett-Packard product can be obtained from your local Sales and Service Office.

Restricted Rights Legend

Use, duplication, or disclosure by the U.S. Government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause in DFARS 252.227-7013.

Hewlett-Packard Company
United States of America

Rights for non-DOD U.S. Government Departments and Agencies are as set forth in FAR 52.227-19(c)(1,2).

Copyright Notices

This product includes software developed by the Apache Software Foundation (http://www.apache.org/). Portions Copyright (c) 1999-2003 The Apache Software Foundation. All rights reserved.

Select Identity uses software from the Apache Jakarta Project including:

- Commons-beanutils.
- Commons-collections.
- Commons-logging.
- Commons-digester.
- Commons-httpclient.

- Element Construction Set (ecs).
- Jakarta-poi.
- Jakarta-regexp.
- Logging Services (log4j).

Additional third party software used by Select Identity includes:

- JasperReports developed by SourceForge.
- iText (for JasperReports) developed by SourceForge.
- BeanShell.
- Xalan from the Apache XML Project.
- Xerces from the Apache XML Project.
- Java API for XML Processing from the Apache XML Project.
- SOAP developed by the Apache Software Foundation.
- JavaMail from SUN Reference Implementation.
- Java Secure Socket Extension (JSSE) from SUN Reference Implementation.
- Java Cryptography Extension (JCE) from SUN Reference Implementation.
- JavaBeans Activation Framework (JAF) from SUN Reference Implementation.
- OpenSPML Toolkit from OpenSPML.org.
- JGraph developed by JGraph.
- Hibernate from Hibernate.org.

Trademark Notices

HP OpenView Select Identity is a trademark of Hewlett-Packard Development Company, L.P.

Microsoft, Windows, the Windows logo, and SQL Server are trademarks or registered trademarks of Microsoft Corporation.

Sun™ workstation, Solaris Operating Environment™ software, SPARCstation™ 20 system, Java technology, and Sun RPC are registered trademarks or trademarks of Sun Microsystems, Inc. JavaScript is a trademark of Sun Microsystems, Inc., used under license for technology invented and implemented by Netscape.

This product includes the Sun Java Runtime. This product includes code licensed from RSA Security, Inc. Some portions licensed from IBM are available at http://oss.software.ibm.com/icu4j/.

IBM, DB2 Universal Database, DB2, WebSphere, and the IBM logo are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both.

This product includes software provided by the World Wide Web Consortium. This software includes xml-apis. Copyright © 1994-2000 World Wide Web Consortium, (Massachusetts Institute of Technology, Institute National de Recherche en Informatique et en Automatique, Keio University). All Rights Reserved. http://www.w3.org/Consortium/Legal/

Intel and Pentium are trademarks or registered trademarks of Intel Corporation in the United States, other countries, or both.

AMD and the AMD logo are trademarks of Advanced Micro Devices, Inc.

BEA and WebLogic are registered trademarks of BEA Systems, Inc.

VeriSign is a registered trademark of VeriSign, Inc. Copyright © 2001 VeriSign, Inc. All rights reserved.

All other product names are the property of their respective trademark or service mark holders and are hereby acknowledged.

Support

Please visit the HP OpenView web site at:

http://openview.hp.com/

There you will find contact information and details about the products, services, and support that HP OpenView offers.

You can go directly to the support web site at:

http://support.openview.hp.com/

The support web site includes:

- Downloadable documentation
- Troubleshooting information
- Patches and updates
- Problem reporting
- Training information
- Support program information

contents

1

Understanding the Connector

The Domino connector enables HP OpenView Select Identity to manage user data in IBM Lotus Notes/Domino systems. The Domino connector is supported on the following Domino versions and platforms:

- Domino 5.0.8 and 5.0.10 on Windows 2000
- Domino 6.0.3 on Solaris 2.8 and 2.9
- Domino 6.5.1 on Windows 2000 and 2003, and on Solaris 2.8 and 2.9

This connector is a two-way connector and pushes changes made to user data in the Select Identity database to the target Domino server. It also enables the agent on the Domino server to send password updates back to Select Identity. The mapping files, which are included with the connector, control how Select Identity fields are mapped to Domino fields.

The Domino connector supports provisioning the following for users on the Domino server:

- Access levels
- Entitlements
- Roles
- User groups

The following describes how the connector works for each provisioning operations:

- Adding a User—
  This functionality adds a user on the Domino server. You can set all of the attributes in the Domino server for the user; this is controlled through configuration of the mapping file.

  An ID file is required for the user to log on to the Domino server using the Notes client. When a Domino administrator creates a user on the Domino Administrator Console, he or she must manually send the ID file to the user. The Domino connector has automated this process.

  When the user is created, the ID file is mailed to the user's mailbox (as specified by the default mail account in Domino server). If an alternative email address is specified for the user (by mapping the AltEmailAddress attribute in the mapping file), the ID file is also mailed to that address. If the AltEmailAddress value is not provided in the mapping file, the connector searches for the value in the `Properties.ini` file, which is installed with the connector's agent on the Domino server. See page 31 for a description of the mapping file attribute, or see Step 5 on page 16 for a description of this property in the `Properties.ini` file.

  Also, when creating users in Select Identity that will be provisioned on a Domino server, keep the following guidelines in mind:

  — The Domino server allows only one ACCESS LEVEL to be specified for a user at a time. Therefore, when creating users in Select Identity, specify only one access level.

  — ENTITLEMENT, ROLE, and Group are multivalue components of the entitlement (for example, a user can belong to zero or more of these attributes). Therefore, you can select any combination of these components when creating the user.

- Modifying a User—
  The connector can modify all the attributes on the Domino server except for the UserID and Password attributes.

  Also, when changing user entitlements in Select Identity for users who are provisioned in Domino, make sure you select only one ACCESS LEVEL. (You may want to remove the ACCESS LEVEL previously selected before adding a new one.)

- Disable Service Membership—
  This removes all entitlements assigned to the user by the Select Identity Service on the Domino server.
- Enable Service Membership—
  This restores all entitlements removed by the Disable Service Membership functionality.
- Delete Service Membership—
  This removes user from the Domino server.
- Disable All Services—
  This functionality disables the user in all Select Identity Services to which he or she is provisioned. This prevents he user from logging in to the Domino server.
- Enable All Services—
  This restores and enables the user for all Services disabled by Disable All Service. On the Domino server, the user can log on to the system once the action completes.
- Reset Password—
  The Domino connector can manage HTTP passwords only; only changes to the user's HTTP password are synchronized with Select Identity. This function resets the user's HTTP password, and the user must specify this new password while using the Notes Web Interface.

2

Installing the Connector

The Domino connector is packaged in the following files:

- `DominoConnector.rar` — contains the binaries for the connector
- `Dominoschema.jar` — contains the following mapping files:
  - `dominouser.properties` — maps the Select Identity user attributes to those on the Domino server
  - `dominogroup.properties` — maps the Select Identity group attributes to those on the Domino server; note that group provisioning is not currently supported, though this file must be extracted during installation
- `DominoAgent.zip` — contains the installation executable for the Domino agent on Windows platforms
- `DominoAgent.tar` — contains the installation executable for the agent on Solaris platforms

These files are located in the `Domino` directory on the Select Identity Connector CD.

Deploying on the Web Application Server

To install the Domino connector on the Select Identity server, complete these steps.

Perform this procedure after the Select Identity product installation. This procedure installs the connector on WebLogic 8.1; you must be familiar with the WebLogic platform.

Also, the J2SE Developer Kit (JDK) version 1.4 must be installed on the application server.

1. Create a subdirectory in the Select Identity home directory, which was created on the application server during the product installation.
2. Copy the `DominoConnector.rar` file to the new subdirectory.
3. Copy the `Dominoschema.jar` file from the Select Identity Connector CD to a temporary folder.
4. Extract the `Dominoschema.jar` file, which contains the mapping files, to the Select Identity home directory.
5. Ensure that the CLASSPATH environment variable that is set in the WebLogic startup script references the Select Identity home directory.
6. Modify the mapping files as needed. The mapping files are described in Understanding the Mapping Files on page 29.
7. Start the application server if it is not currently running.
8. Log on to the WebLogic Server Console.
9. Navigate to ***My_domain*** → **Deployments** → **Connector Modules**.
10. Click **Deploy a New Connector Module**.
11. Locate and select the `DominoConnector.rar` file from the list. It is stored in the connector subdirectory in the Select Identity home directory.
12. Click **Target Module**.
13. Select the **My Server** (your server instance) check box.
14. Click **Continue**. Review your settings.
15. Keep all default settings and click **Deploy**.

    The Status of Last Action column should display Success.

After installing the connector, log on to the Select Identity client and deploy the connector using the Connector pages. Then, create a resource that represents the connector, and configure a Service that relies on the Domino resource. See the *HP OpenView Select Identity Administrator Guide* for procedures. The Resource Access Information appendix provides detailed information about creating a Domino resource.

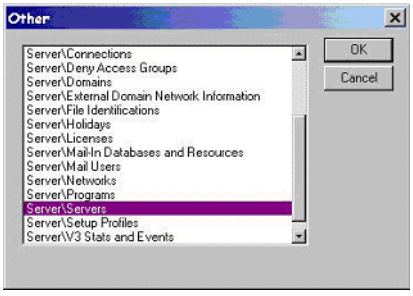
Installing the Agent on the Domino Server

This is an agent-based connector. The agent is a suite of Services and support files deployed on the resource. Use the following procedures to install and configure the agent on the Domino server.

Configuring Domino Security Settings

The following procedure describes how to configure security settings on the Domino server (versions 5.0.8, 5.0.10, and 6.5.1) running on Windows or Solaris. You must complete these steps to run the agent, which is Java-based, for reverse synchronization.

1. Verify that the Domino server is running.
2. Launch the Domino Administrator.
3. Modify the security settings for the server, as follows:
   a. Select **View** → **Server** → **Other**. The Other dialog is displayed.



   b. Select **Server/Servers** from the list and click **OK**. The Domino Address Book - Server/Servers dialog is displayed.

c Click **Edit Server**.

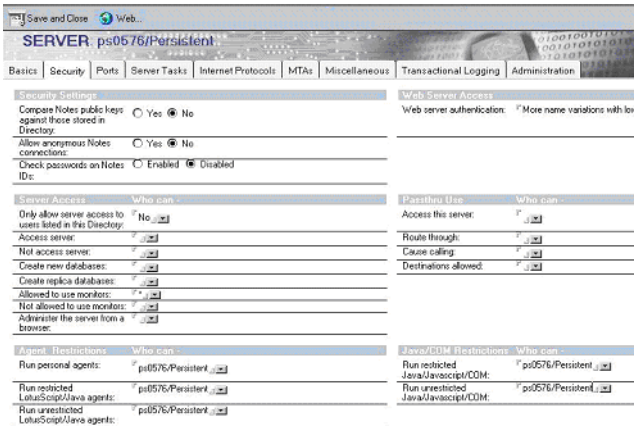
d Select the **Security** tab.

e Navigate to the Server Access section on the Security tab and select the **users listed in all trusted directories** option. In the And section, select the account (*server_name/domain_name*).

f If you are running Domino 5.0.8 and 5.0.10, locate the Agents Restriction section of the Security tab and edit the following settings to include the Administrator account and Server account (*server_name/domain_name*) on the Domino server:

- Run personal agents
- Run restricted LotusScript/Java agents
- Run unrestricted LotusScript/Java agents
- Run restricted Java/JavaScript/COM
- Run unrestricted Java/JavaScript/COM

The following illustrates the Domino 5.0.*x* security settings:

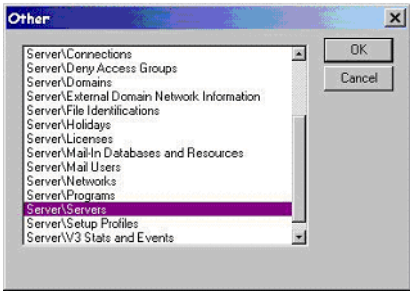


g If you are running Domino 6.5.1 on Windows, locate the Programmability Restrictions section of the Security tab and edit the following settings to include the Administrator account and Server account (*server_name/domain_name*) on the Domino server:

- Run Unrestricted methods and operations
- Run Restricted Lotus script/Java Agents

4 Modify the preferred `Notes.ini` settings, as follows:

a Select **View** → **Server** → **Other**. The Other dialog is displayed.



b Select **Server/Servers** from the list and click **OK**. The Domino Address Book - Server/Servers dialog is displayed.

c Select **Configuration** → **Servers** → **Configurations**.

d Select the server name.

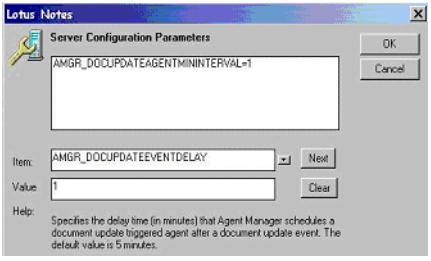
e Click **Edit Configuration**.

f Click the **NOTES.INI Settings** tab.

g Click **Set/Modify Parameters**.

h Specify **1** as the value of AGMR_DOCUPDATEAGENTMININTERVAL and click **Next** (on 5.*x*) or **Add** (on 6.*x*).

i Specify **1** as the value of AGMR_DOCUPDATEEVENTDELAY and click **Next** (on 5.*x*) or **Add** (on 6.*x*).

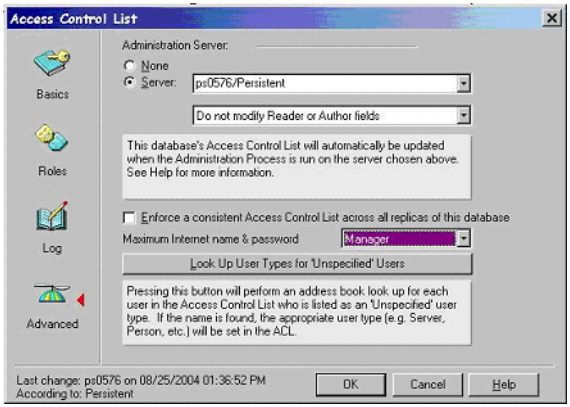


j Click **OK** to close the dialog.

k Save your settings and close the Other dialog.

5 To set access control settings, which enable the connector to perform operations related to roles and entitlements, complete these steps:

a Select **File** → **Database** → **Access Control**. The Access Control List dialog is displayed.



b Click **Advanced** on the left side of the dialog.

c Select **Manager** from the Maximum Internet name & password drop-down list.

d Click **OK** to close the dialog.

Installing the Agent on Windows

Perform the following to install the agent on Windows:

1 Edit the CLASSPATH environment variable to append the installation folder of the Domino server and the location of the `Notes.jar` file. Also, ensure that the `bin` folder of the JDK is included in the PATH environment variable.

For example, if the Domino server is installed in C:\Lotus and the JDK resides in C:\jdk141_05, the CLASSPATH variable should include the following:

```
C:\Lotus\Domino\Notes.jar;C:\Lotus\Domino;
C:\jdk141_05\bin;
```

2 Copy the `DominoAgent.zip` file from the Select Identity Connector CD to a folder on the Domino server.

3 Extract the `DominoAgent.zip` file to a folder where you wish to install the Domino agent. A folder named `DominoAgent` is created.

4 Move the `Properties.ini` and `opAttributes.properties` files from the `DominoAgent\config` folder to the installation folder of the Domino server (such as `C:\Lotus\Domino`).

5 Modify the `Properties.ini` file to configure the agent with the necessary access information. The following table describes the properties to set in the file:

Property	Default	Description
PORT	5002	The port number on which the agent will be listening for requests.
CHECK_LOGIN	true	Whether the agent should verify the logon credentials with the Domino server.
CONCERO_ SERVER_URL	http:// myserver:7001/lmz/ webservice	URL to the Web Service on the Select Identity server, which listens for reverse notifications. Typically, the format of the URL is **http://*server*:*port*/lmz/ webservice**.
AltEmailAddress	CN=Administrator /O=Domain	The administrator's email address. When a user is added, the ID files will be emailed to this account if the user model does not have this property.
MAX_LOGIN_ RETRIES	3	Number of retries for the entering logon credentials.
DATABASE_ NAME	Names.nsf	Database name for reverse notification. The modification details are retrieved from this database.

CONCERO_ SERVER_URL	http:// myserver:7001/lmz/ webservice	URL to the Web Service on the Select Identity server, which listens for reverse notifications. Typically, the format of the URL is **http://*server*:*port*/lmz/ webservice**.
AltEmailAddress	CN=Administrator /O=Domain	The administrator's email address. When a user is added, the ID files will be emailed to this account if the user model does not have this property.
MAX_LOGIN_ RETRIES	3	Number of retries for the entering logon credentials.
DATABASE_ NAME	Names.nsf	Database name for reverse notification. The modification details are retrieved from this database.

Here are the contents of an example `Properties.ini` file:

```
PORT=5003
CHECK_LOGIN=true
CONCERO_SERVER_URL=http://domino_svr1:7001/lmz/webservice
AltEmailAddress=CN=Administrator/O=Domain
MAX_LOGIN_RETRIES=3
DATABASE_NAME=Names.nsf
```

6 Modify the `opAttributes.properties` file, which provides operational attributes that are sent to the Select Identity server during reverse synchronization requests. The file must contain the following:

- Logon credentials —
  Set the urn:oasis:names:tc:SPML:1:0#UserIDAndOrDomainName and urn:trulogica:concero:2.0#password keys to provide the user name and password need to authenticate with the Select Identity server.
- The name of the Domino resource in Select Identity —
  Set the urn:trulogica:concero:2.0#resourceId key.

- The reverse synchronization key —
  Set the urn:trulogica:concero:2.0#reverseSync key to true.

Here are contents of an example `opAttributes.properties` file:

```
urn:oasis:names:tc:SPML:1:0#UserIDAndOrDomainName=sisa
urn:trulogica:concero:2.0#password=abc123
urn:trulogica:concero:2.0#resourceId=Domino510
urn:trulogica:concero:2.0#reverseSync=true
```

7. Edit the `startDominoApp.cmd` file to replace the $domino_home string with the absolute path to the folder containing the `Notes.jar` file. For example, this file might reside in `C:\Lotus\Domino`.
8. Start the agent by entering **`startDominoApp.cmd`** from a Command Prompt.
9. When prompted, provide the Domino Administrator's user name and password.

To stop the agent at any time, enter **`Exit`** in the Command Prompt window running the agent.

After you install the agent on Windows, the following folders and files are available:

install_dir\	`startDominoApp.cmd`	Starts the agent.
*install_dir**bin*\	`dominoapp.jar`	The main application JAR file. This file is included in the CLASSPATH.
	`connagents.jar`	The JAR file containing the Domino agents.
*install_dir**config*\	`commons-logging.properties`	The configuration file for the logging libraries in `commons-logging.jar`. This file is included in the CLASSPATH.
	`log4j.properties`	The configuration file for the logging libraries in `log4j-1.4.8.jar`. This file is included in the CLASSPATH.

install_dir\lib\	commons-logging.jar	Logging libraries. This file is included in the CLASSPATH.
	log4j-1.2.8.jar	Logging libraries. This file is included in the CLASSPATH.
	xercesImpl.jar	Xerces XML parser libraries. This file is included in the CLASSPATH.
	xmlParserAPIs.jar	Xerces XML parser libraries. This file is included in the CLASSPATH.

Installing the Agent on Solaris

Complete the following steps to install the agent on the Domino server:

1. Log on to the Solaris system as the same user who installed the Domino server.
2. Export the CLASSPATH environment variable and ensure that it includes the path to the Domino installation directory, the path to the `Notes.jar` file, and the path to the JDK `bin` directory.

   For example, if Domino is installed in /usr/lotus and the JDK resides in /usr/jdk141_05, the CLASSPATH variable will include the following:

   `/usr/lotus/Domino/Notes.jar: /usr/lotus/Domino: /usr/jdk141_05/bin:`
3. Copy the `DominoAgent.tar` file from the Select Identity Connector CD to a directory on the Domino server.
4. Extract the `DominoAgent.tar` file, which creates the required directory structure.
5. Move the `Properties.ini` and `opAttributes.properties` files from the directory to the Domino Data Directory, which is typically `/usr/lotus/notesdata` or `/lotus/notesdata`.

6 Modify the `Properties.ini` file to configure the agent with the necessary access information. See Step 5 on page 16 for details about this file.

7 Modify the `opAttributes.properties` file, which provides operational attributes that are sent to the Select Identity server during reverse synchronization requests. Step 6 on page 17 for details about this file.

8 Edit the `startDominoApp.sh` file to ensure that the following variables are set according to the Domino server installation:

Variable	Default Value	Description
DOMINO_LIBRARY _PATH	/var/lotus/notes/ 65010/sunspa	Location of the Domino libraries (including `Notes.jar`)
DOMINO_JAVA _PATH	/var/lotus/bin	Location of the Java executable used by Domino
NOTES_DATA _DIRECTORY	/usr/local/notesdata	Location of the Notes components (such as `Notes.ini`)
COMMANAGER _PATH	/export/home/notes/ Select_Identity	Location of the directory where the contents of the `DominoAgent.tar` file where extracted

9 Start the agent by running the following command from the command line:

```
sh startDominoApp.sh
```

10 When prompted, provide the Domino Administrator's user name and password.

11 Copy `connagent.jar` from DominoAgent/bin to the system where the Domino Administration client is installed.

After you install the agent on Solaris, the following directory structure and files are available:

install_dir/	`startDominoApp.sh`	Starts the agent.
install_dir/bin/	`dominoapp.jar`	The main application JAR file. This file is included in the CLASSPATH.
	`connagents.jar`	The JAR file containing the Domino agents.
install_dir/config/	`commons-logging.properties`	The configuration file for the logging libraries in `commons-logging.jar`. This file is included in the CLASSPATH.
	`log4j.properties`	The configuration file for the logging libraries in `log4j-1.4.8.jar`. This file is included in the CLASSPATH.
install_dir/lib/	`commons-logging.jar`	Logging libraries. This file is included in the CLASSPATH.
	`log4j-1.2.8.jar`	Logging libraries. This file is included in the CLASSPATH.
	`xercesImpl.jar`	Xerces XML parser libraries. This file is included in the CLASSPATH.
	`xmlParserAPIs.jar`	Xerces XML parser libraries. This file is included in the CLASSPATH.

Configuring Password Synchronization in Domino 5.0.*x*

The following procedure configures the agent installed on the Domino 5.0.8 and 5.0.10 server, enabling the agent to perform password synchronization.

1. Replace the `Form5.nsf` file that resides in the `\Domino\Data\iNotes` folder with the `Form5.nsf` file provided by Select Identity. The new `Form5.nsf` file is packaged in `passwordSync_5_0_X.zip`, which was extracted from the `DominoAgent.zip` file.

   If the `Form5.nsf` file that resides in `\Domino\Data\iNotes` was previously modified by an administrator, contact your HP OpenView Select Identity representative. Replacing this file with the one provided by Select Identity will overwrite the changes.

2. Start the Domino server by selecting **Start** → **Programs** → **Lotus Applications** → **Lotus Domino Server**.
3. Launch Domino Designer by selecting **Start** → **Programs** → **Lotus Applications** → **Lotus Domino Designer**.
4. Open the iNotesMail and C&S template.
5. Select **File** → **Database** → **Open**. This displays the Open Database dialog.
6. Enter the following information on this dialog:
   - For Server, enter **`local`**.
   - For Database, enter **`iNotes Mail and C&S`**.
   - Ensure that **`iNotes5.nsf`** is listed in the Filename field.
7. Select **View** → **Agents**, which displays the agent dialog.
8. Click **New Agent**.
9. Provide the following information in the dialog:
   - Specify any name, such as **`TAPassAgent`**, in the Name field.
   - Select the **Shared** option.
   - Select **Manual from agent list** for the When should this Agent run on? setting.
   - Select **runonce at command** for the Which document should it act on? setting.

— Select **Imported Java** from the Action drop-down list, then provide this information:

– Click **Import Class Files**.

– Enable **Archive** in Show Files.

– Browse to the agent's installation folder, select **connagents.jar**, and click **Add/Replace Files**.

– Set the base class to **`[com/trulogica/domino/connagents/PwChange.class]`**.

10 Save the settings and close the dialog.

11 On the agent window, enable **Web Agent**.

12 Ensure that the Runtime Security Level option is set to **2. Allow restricted Operations**.

13 Close Domino Designer.

Configuring Password Synchronization in Domino 6.*x*

Complete the following steps to configure the Select Identity agent in Domino 6.0.8 or 6.5.1:

1 Replace the `Form5.nsf` and `Form6.nsf` files that reside in the `\Domino\Data\iNotes` folder with the `Form5.nsf` and `Form6.nsf` files provided by Select Identity. The new files are packaged in `passwordSync_6_5_1.zip`, which was extracted from the `DominoAgent.zip` file.

If the `Form`*X*`.nsf` file that resides in `\Domino\Data\iNotes` was previously modified by an administrator, contact your HP OpenView Select Identity representative. Replacing this file with the one provided by Select Identity will overwrite the changes.

2 Launch Domino Designer by selecting **Start** → **Programs** → **Lotus Applications** → **Lotus Domino Designer**.

3 Open the Domain Address Book database by selecting **File** → **Database** → **Open**. The Open Database dialog is displayed.

4 Enter the following information:

— Choose the correct server (typically *machine_name/domain_name*) from the Server list.

— Select **iNotes Web Access (R5)** from the Database list if using the Forms5 template, or select **Domino Web Access (6)** if using the Forms6 template.

— Ensure that **`iNotes5.ntf`** is specified in the Filename field if using the Form5 template, or ensure that **`iNotes6.ntf`** is specified if using the Form6 template.

5 Select **Recent Databases** → **Shared Code** → **Agents** → **New Agent**. The Agent properties dialog is displayed.

6 Enter the following information:

— On the first tab:

– Specify any name, such as **`TAPassAgent`**, in the Name field.

– Select the **Shared** option.

– Select **On Event** for the Trigger setting.

– Select **Agent List Selection** for the Runtime setting.

– Select **None** for the Target setting.

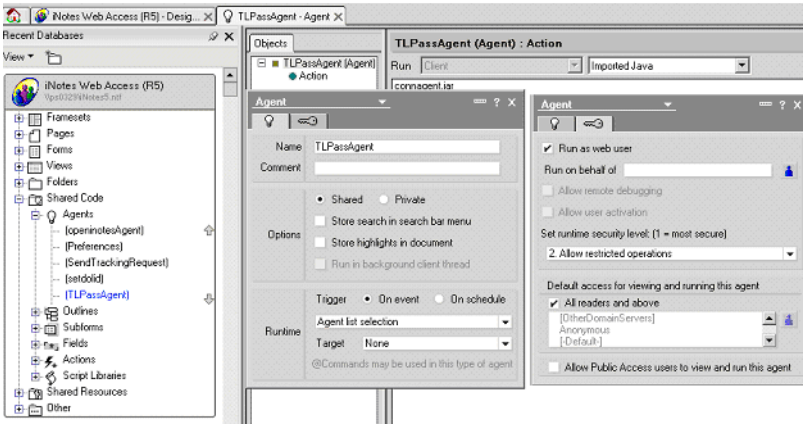
— On the second tab:

– Select the **Run as web user** option.

– Select **2 Allow Restricted operations** for the Set runtime security level setting.

– Select **All readers and above enabled** for the Default Access for Viewing and running the agent setting.

The following illustrates the settings:



7 Select **Imported Java** from the Action drop-down list, then provide this information:

— Click **Import Class Files**.

— Enable **Archive** in Show Files.

— Browse to the agent's installation folder, select **connagents.jar**, and click **Add/Replace Files**.

— Set the base class to **`[com/trulogica/domino/connagents/PwChange.class]`**.

8 Close Domino Designer.

Upgrading Users' Mail Templates

To enable Domino to use the new template file for all new users, edit the `Notes.ini` file located in C:\Lotus\Domino to change the DefaultMailTemplate entry. Replace `mail50.ntf` with the name of the iNotes template (`iNotes5.ntf` or `iNotes6.ntf`). Therefore, the entry will look like this:

```
DefaultMailTemplate=iNotes6.ntf
```

Then, perform the procedures in this section only if you have created users on the Domino server using Select Identity prior to configuring Domino to use the new template (`iNotes5.ntf` or `iNotes6.ntf`).

Activating password synchronization for Domino users requires that the users migrate to the new (modified) iNotes template. They must also use the iNotes Web Interface to change their Internet password. There are two ways to migrate the user mail template; however, user interaction is required whichever method is used.

Administrator Initiated Upgrade

As the Administrator, you can perform the following steps to initiate the migration of legacy users to the new iNotes template:

1. Open the Domino Administrator.
2. Select the users to migrate from the People list.
3. Right-click and select **Upgrade**. A new form is displayed.
4. Click the **Software Distribution** tab.
5. In the New mail template file name field, enter the path to the new iNotes template provided by Select Identity (`iNotes5.ntf` if using iNotes 5 on Domino 5.0.*x* or Domino 6.*x* or `iNotes6.ntf` if using iNotes 6 on Domino 6.*x*).
6. Send the mail.
7. Inform the user of the following steps, which he or she must perform after receiving the email:
   - — Open the Notes mail client.
   - — Open the mail received from the administrator.
   - — Click the **Upgrade** button. This initiates the upgrade process.
   - — Provide the Notes ID password when prompted.

   The user's mailbox will be migrated to the new iNotes template.

User Initiated Upgrade

Users can perform the following steps to migrate their mailboxes to the new iNotes template. Instruct the users to perform the following steps:

1. Open his or her mailbox using the Notes client program.
2. Select **File** → **Database** → **Replace Design**, then select the Template Server to the Domino Server.

3 Select the **Show Advanced templates** option.

4 Complete one of the following steps based on the version of Domino:

— If using iNotes 5 on Domino 5.*x*, select **iNotes Mail and C&S** from the list. `iNotes5.ntf` is displayed next to the About button.

— If using iNotes 5 on Domino 6.*x*, select **iNotes Web Access**. `iNotes5.ntf` is displayed next to the About button.

— If using iNotes 6 on Domino 6.*x*, select **Domino Web Access**. `iNotes6.ntf` is displayed next to the About button.

5 Click the **Replace** button to migrate the mailbox to the selected iNotes template.

Changing Passwords Using the Web Client

After you configure the default user template (by replacing `iNotes5.ntf` or `iNotes6.ntf`), users can perform the following steps to synchronize their passwords with the Select Identity server. Instruct your users to log on to the iNotes Web Access interface and change their passwords, enabling Domino to save the new Internet passwords. Before sending this procedure to users, substitute your values for variables in the procedure, such as the Domino server name.

Provide the following steps to your users:

1 Launch Internet Explorer and load the following URL:

http://*domino_server_name*/mail/*username*.nsf

where *username* is the user's name in Domino/Notes. The Network Password page is then displayed.

2 Enter your user name (short name) and Password. The iNotes Web Access page is displayed.

3 Click **Preferences**.

4 Click **Save and Close** to close the Preferences page. You are returned to the iNotes Web Access page.

5 Again, click **Preferences**.

6 Click **Change** under Change Internet Password.

7 On the Change Password dialog, enter your old password and a new password. Then, close the dialog.

8 Close the Preferences page.

9 Click **Logout** to log out of the iNotes Web Access pages.

3

Understanding the Mapping Files

The Domino connector is deployed with the following mapping files:

- `dominouser.properties`
- `dominogroup.properties`

These files contain the attributes required by the resource. The files are used to map user and group account additions and modifications from Select Identity to the Domino server. When you deploy a resource through the Resources pages on the Select Identity client, you can review these files.

Note that the `dominogroup.properties` file is installed with the Domino connector and must be present on the system, but group provisioning is not supported at this time.

You can create attributes that are specific to Select Identity using the Attributes pages on the Select Identity client. You can then use these attributes to associate Select Identity user accounts with system resources by mapping the attributes in the mapping files described in this chapter. This process becomes necessary because, for example, a single attribute “username” can have a different definition on three different resources, such as “login” for UNIX, “UID” for a database, and “userID” on a Windows server.

You do not need to edit this file unless you want to map additional attributes to your resource. If attributes and values are not defined in the mapping files, they cannot be saved to the resource through Select Identity. The

dominouser.properties file is a text file that maps each Select Identity user attribute to an attribute on the resource; the attributes are delimited by |. Consider this excerpt:

```
UserId|UserId
```

The Select Identity user attribute is named UserId and it is mapped to the UserId attribute on the Domino resource. In this case, the attributes have the same name, though often they do not.

Attributes can be concatenated. The attribute names and the separators must not contain the | delimiter. For concatenation, the format is as follows:

```
[<SI Attribute>]<separator>[<SI Attribute>]|<Resource Attribute>
```

as in this example:

```
[addr1] [addr2]|HomePostalAddress
```

where addr1 and addr2 are attributes in Select Identity. They are concatenated to form the value of the HomePostalAddress attribute on the resource. A space is used as a separator between the two Select Identity attributes.

The dominouser.properties file provides the mandatory mappings that must be configured for Select Identity to provision users on the Domino server. The primary key is UserId; this Domino attribute must be mapped to a Select Identity attribute in order for user information to be stored on the Domino server. It should be the first entry in dominouser.properties.

You can edit the Select Identity resource attributes; they reflect the identity information as seen in Select Identity. The physical resource attributes are literal attributes of user accounts on Domino. These attributes cannot be changed. The following table provides a list of all Domino attributes that you can map if you wish to provision users with this information. Here is a description of the columns provided in the table:

- **Select Identity Resource Attribute**— The attribute used by the Domino connector, as defined in the mapping file.
- **Domino User Attribute —** The name of the attribute on the Domino server.
- **Label on Domino UI** — The name of the property on the Domino UI that corresponds to the attribute on the Domino server.
- **Description** — A description of the attribute and any noteworthy information needed when assigning values to the attribute.

The mandatory attributes that are mapped by default are noted.

Select Identity Resource Attribute	Domino User Attribute	Label on Domino UI	Description
UserId	UserId	Short name/ UserID (on the Basics tab)	Primary key for the connector, and this is a mandatory attribute.
Password	Password	(not available in UI)	This is a mandatory attribute.
AltEmail Address	AltEmail Address	(not available in UI)	An alternative email address where Select Identity will send the user's ID file.
FirstName	FirstName	First name (on the Basics tab)	
MiddleInitial	MiddleInitial	Middle initial (on the Basics tab)	
LastName	LastName	Last name (on the Basics tab)	
Title	Title	Personal title (on the Basics tab)	
JobTitle	JobTitle	Job title (in Work Details on the Work tab)	
CompanyName	CompanyName	Company (in Work Details on the Work tab)	
Manager	Manager	Manager (in Work Details on the Work tab)	

Select Identity Resource Attribute	Domino User Attribute	Label on Domino UI	Description
OfficePhone Number	OfficePhone Number	Office phone (in Work Details on the Work tab)	
CellPhone Number	CellPhone Number	Cell phone (in Work Details on the Work tab)	
OfficeCity	OfficeCity	City (in Company Information on the Work tab)	
OfficeState	OfficeState	State/Province (in Company Information on the Work tab)	
City	City	City (on the Home tab)	
State	State	State/province (on the Home tab)	
Zip	Zip	Zip/postal code (on the Home tab)	
HomePostal Address	HomePostal Address	Street address (on the Home tab)	
HomePhone Number	PhoneNumber	Home phone (on the Home tab)	
Comment	Comment	Comment (on the Miscellaneous tab)	

Select Identity Resource Attribute	Domino User Attribute	Label on Domino UI	Description
(not mapped by default)	Suffix	Generational qualifier (on the Basics tab)	
(not mapped by default)	CheckPassword	Boolean for Change Password (on the Basics tab)	
(not mapped by default)	MailSystem	Mail System (on the Mail tab)	
(not mapped by default)	MailDomain	Domain (on the Mail tab)	
(not mapped by default)	MailServer	Mail Server (on the Mail tab)	
(not mapped by default)	MailFile	Mail file (on the Mail tab)	
(not mapped by default)	MailAddress	Forwarding address (on the Mail tab)	
(not mapped by default)	Internet Address	Internet address (on the Mail tab)	
(not mapped by default)	Message Storage	Format preference for incoming mail (on the Mail tab)	
(not mapped by default)	Encrypt IncomingMail	Encrypt incoming mail (on the Mail tab)	
(not mapped by default)	ccMail Location	CC Mail Location (on the Mail tab)	

Select Identity Resource Attribute	Domino User Attribute	Label on Domino UI	Description
(not mapped by default)	ccMailUser Name	CC Mail Username (on the Mail tab)	
(not mapped by default)	Department	Department (in Work Details on the Work tab)	
(not mapped by default)	EmployeeID	Employee ID (in Work Details on the Work tab)	
(not mapped by default)	Location	Location (in Work Details on the Work tab)	
(not mapped by default)	OfficeFAX PhoneNumber	FAX phone (in Work Details on the Work tab)	
(not mapped by default)	PhoneNumber_6	Pager number (in Work Details on the Work tab)	
(not mapped by default)	Assistant	Assistant (in Work Details on the Work tab)	
(not mapped by default)	OfficeStreet Address	Street address (in Company Information on the Work tab)	
(not mapped by default)	OfficeZIP	Zip/postal code (in Company Information on the Work tab)	
(not mapped by default)	OfficeCountry	Country (in Company Information on the Work tab)	

Select Identity Resource Attribute	Domino User Attribute	Label on Domino UI	Description
(not mapped by default)	OfficeNumber	Office Number (in Company Information on the Work tab)	
(not mapped by default)	Country	Country (on the Home tab)	
(not mapped by default)	HomeFAXPhone Number	FAX phone (on the Home tab)	
(not mapped by default)	Spouse	Spouse (on the Home tab)	
(not mapped by default)	Children	Children (on the Home tab)	
(not mapped by default)	PersonalID	Personal ranking (on the Corporate Hierarchy Information tab)	
(not mapped by default)	x400Address	Other X.400 address (on the Miscellaneous tab)	
(not mapped by default)	Calendar Domain	Calendar domain (on the Miscellaneous tab)	
(not mapped by default)	WebSite	Web page (on the Miscellaneous tab)	

Select Identity Resource Attribute	Domino User Attribute	Label on Domino UI	Description
(not mapped by default)	PublicKey	Notes certified public key (on the Notes Certificates tab)	
(not mapped by default)	Certificate	Internet certificate (on the Internet Certificates tab)	
(not mapped by default)	Owner	Owners (on the Administration tab)	
(not mapped by default)	AltFullName	Alternate FullName (on the Administration tab)	
(not mapped by default)	AltFullName Sort	Alternate FullName Sort (on the Administration tab)	
(not mapped by default)	LocalAdmin	Administrators (on the Administration tab)	
(not mapped by default)	Password Digest	Password digest (on the Administration tab)	

Select Identity Resource Attribute	Domino User Attribute	Label on Domino UI	Description
(not mapped by default)	Password ChangeDate	Password Change date (on the Administration tab)	
(not mapped by default)	Password Change Interval	Password Change Interval (on the Administration tab)	
(not mapped by default)	PasswordGrace Period	Password Change Grace Period (on the Administration tab)	
(not mapped by default)	ClientType	Notes client license (on the Administration tab)	
(not mapped by default)	Profiles	Setup profile(s) (on the Administration tab)	
(not mapped by default)	AvailableFor DirSync	Foreign directory synch allowed (on the Administration tab)	
(not mapped by default)	NetUserName	Network account name (on the Administration tab)	

Select Identity Resource Attribute	Domino User Attribute	Label on Domino UI	Description
(not mapped by default)	ProposedAlt CommonName	Proposed alternate common name (on the Administration tab)	
(not mapped by default)	ProposedAlt OrgUnit	Proposed alternate unique organizational unit (on the Administration tab)	
(not mapped by default)	Proposed AltFull NameLanguage	Proposed alternate name language (on the Administration tab)	
(not mapped by default)	Sametime Server	Sametime server (on the Administration tab)	

4

Uninstalling the Connector

If you need to uninstall a connector from Select Identity, make sure that the following are performed:

- All resource dependencies are removed.
- The connector is deleted through the Connectors home page on the Select Identity client.

Uninstalling the Domino Connector

Perform the following to delete the Domino connector from the Select Identity server:

1. Log on to the WebLogic Server Console.
2. Navigate to ***My_Domain*** → **Deployments** → **Connector Modules**.
3. Click the delete icon next to the connector that you want to uninstall.
4. Click **Yes** to confirm the deletion.
5. Click **Continue**.

Uninstalling the Domino Agent

Perform the following steps to delete the agent on the Domino server:

1. Delete the directory where the `DominoAgent.zip` or `DominoAgent.tar` file was extracted.
2. Delete the `opAttributes.properties` and `Properties.ini` files from `C:/Lotus/Domino`.
3. Remove the `Forms5.nsf` or `Forms6.nsf` file that was copied during installation.
4. Delete the password synchronization agent that was created in Domino Designer.